(Public links to this specific article: http://korova.com/virus/.)

An Internet SPAM/HOAX/CHAIN email primer:

The Internet. Who'd have known it would become the hula hoop of the Nineties? Everyone's talking about it, everyone wants it, and everyone loves it.

E-mail is considered the premier Internet, and intranet, application. As users become increasingly comfortable with e-mail tools, they begin to use it for more business (and non-business) uses. Some of the social uses regularly include sharing jokes, "nice to know informational tidbits," … and dire warnings of digital doom. The electronic town square has been used (and abused) as ordinary folks take it upon themselves to "pass the word" about notorious rumors and shocking tales.

This page is organized into four sections:

'Net rumors (What they are, how to recognize them)
The "e-v-mail" (the theory as to why 'Net rumors are so popular, and some remedies)
At Work (issues to be considered from your professional e-mail account)
At Home (issues to be considered when you get 'Net rumors from friends)

'Net Rumors

Unfounded hearsay on the Internet, or 'Net rumors, appear in various forms, including these:

Virus hoaxes

The idea of a virus hoax is said to originate with a satirical post about a reputed 2400 baud virus* that actually duped some journalists (who then passed the fraud on as legitimate). Some argue that the Michelangelo virus scare of 1992* was a gross hype of a minimal risk that the media swallowed whole and spammed across the airwaves ... enabling McAfee and Symantec to sell tons of antivirus software to frightened PC users. Virus hoaxing gained true grass roots popularity with Good Times* on America Online. AOL is well-suited for newbie users, so frantic hoax hysteria spreads like wildfire on the service. Unfortunately for the rest of the online world, Good Times took off on the Internet, spawning a dozen or more imitations.

Aside from some fanciful elaborations of computer paranoia, most virus warnings are lame jokes that require more suspension of disbelief than computer naiveté.

* [Virus definitions courtesy of the Computer Virus Myths home page.]

Chain e-mail

Like old-fashioned chain letters through the snail mail, chain e-mail asks (sometimes demands) that you forward copies to everyone else you know, or horrible things will happen. Named for ... I don't know, but chain e-mail has this long "chain" of mail forwards on it, usually because no one even stops to think or remove mail headers before clicking the FORWARD button. (It's probably a great way for spammers to harvest strangers' e-mail addresses.) The result? A HUGE mail message with little or no real content.

"Forwardables"

Community action can be a wonderful thing, but the Internet makes it too easy, particularly to spread false requests, and unfounded fears. The "Forwardables" strain includes requests to send postcards to terminally ill children, contest announcements, class action suits, and please to save public institutions like the NEA or NPR. Of course, in addition to saving yourselves, you're asked to save the rest of the world: "please, please,
forward this" to everyone you know.

A new breed of Forwardable is the "compliance," or direct-threat, warning. It insists that you forward the e-mail (or ICQ message, a new form of instant messaging) to everyone you know ... or dire circumstances will befall you or your computer. In the spring of 1998, ICQ messages with Web URLs attached started spreading. The recipient was directed to forward the ICQ message to "everyone on your contact list" or else "you will be kicked off ICQ." Actually, according to Mirabilis, no such action is being contemplated, and any such announcement would arrive as a system message, not a distributed chain message. (See the AOL Hacker Riot II and "Andy Death Threat" hoaxes.) (Why would someone start a chain message to generate hits on a web page? Often these web pages feature banner ads. It's possible that the webmaster has arranged for payment based on "page views," in which just generating hits for the page containing the banner is all that is needed to receive a fee. Artificially boosting the page views can translate directly to revenue.)

This variety of message clearly features the three elements that the CIAC Chain Letter page calls The Hook, The Threat, and The Request. Put simply, such a message portrays a danger, asserts that the danger can happen to YOU, and the only thing you can do to help is to forward the message on. These messages rarely encourage you to check the facts with a reputable, objective source of information. This is often because there is no reputable, objective source to confirm the message's inaccurate claims!

Cyberban Legends

Similar to chain e-mail and "Forwardables," these dire warnings tell tales of doom and disaster befalling ordinary folks, sometimes even FOAFs (friend of a friend). As often as not, they're well-known urban legends, "scarelore" running rampant through promiscuous Inboxes. Online, I call these "Cyberban Legends."

The "e-v-mail"

I lump most of these types of impersonal, spammed e-mail as "e-v-mail," or electronic virus mail. Why? They can all credit their success to the concept of a thought virus (see below). The thought virus is essentially that idea, buried inside the e-mail, which causes a user to forward it frivolously, needlessly infecting others. Some users are notorious carriers of the thought virus, regularly spamming others with forwarded mail.

The Thought Virus (meme)

The Cure (vaccine)

"... An opportunistic self-replicating e-mail virus which tricks its host into replicating it, sometimes adding as many as 200,000 copies at a go. It works by finding hosts with defective parsing apparatus which prevents them from understanding that a piece of e-mail which says there is an e-mail virus and then asking them to remail the message to all their friends is the virus itself."

Clay Shirkey
Les Jones' Good Times Virus Hoax FAQ

"... The false belief is the real virus. As a thought contagion, it is a meme that manipulates you to retransmit rather than an actual computer virus infecting computers. The real 'host computer' is the human brain, and a population of brains interconnected by the Internet provides the susceptible medium for pandemic thought contagions."

Aaron Lynch
Thought Contagion Analyst
CC: Contagious Correction

"... sometimes people will foolishly send out their own paraphrase of an alert, perhaps based on something they heard verbally. These second-hand alerts usually contain exaggerations and other factual inaccuracies,...."

Phil Agre
Department of Information Studies
UCLA
Designing Effective Action Alerts For the Internet

At Work

The business impact can be far worse than the annoyance we feel at home. Negative impacts in the workplace can include:

> a. Users' inboxes are clogged with unsolicited warnings of dubious origin. Time and resources are squandered for a non-business activity.

> b. Mail servers are overloaded with multiple copies of redundant, incorrect information that does not contribute a business value; it's "spam" in the workplace. It can even crash a mail server.

> c. Notifications don't come from competent IS personnel within the organization. Instead, they're spread around like the seasonal cold, taking out half the staff on one shot.
> d. Possibly the most threatening danger is that when hoaxes are forwarded by employees using their business e-mail addresses, the hoax can gain considerable "authenticity" by virtue of the relay header. So if user Joe Blau at Computer Security Solutions gets the Join the Crew virus hoax, and then spams it to 250 of his best friends on the net, the forwarded message (with his very authoritative domain and organization fields) gains remarkable credibility. Never mind that Joe happens to be a summer intern in the game-testing unit. [See Rob Rosenberger's excellent article on the "False Authority Syndrome".]

In all my recent computer security discussions, I've recommended the policy that all virus alerts, warnings, and chain mail should be forwarded to the computer administration staff for evaluation. Bona fide threats and bulletins should originate in an organization only from the authorized parties within a technical support or computer security staff. This limits the frivolous use of company resources, and also promotes a process in which only valid information is disseminated, through proper channels.

If you receive e-mail at work like that described above, the first reasonable step is to forward it only to the company's computer staff (alternately called Information Technology, Information Services, Network Support, Network Administration). Let them track down the truth while you go on about your real work.

[As of January 1, 1999, several of the liabilities that I mentioned above have since come true for the American Chemical Society and the United States Post Office, no kidding. I hate to say I told you so....]

If you're a computer security professional or public information officer, drafting an e-mail warning or alert, I invite you to read my Drop-dead Internet Alerts page. It provides unbeatable tips for writing an effective Internet alert.

At Home

As for home users. Well. Sending out false information and bogus warnings aren't the actions we anticipate from friends. So why do it ourselves?

Many of this site's visitors tell me that it's a very real burden when coworkers, friends and family members include them in the problem. Here are some recent examples from Korova.com's mailbox:

David, this one came today from a friend, forwarded to him from his friend.

I hate it when friends and relatives send me this stuff.

I seem to be getting alot of these lately, both at work and at home. Here's another one.

I am sure I am going to see this "hoax" email in my in box for months unless it is stopped now.

I hope it ceases soon. I am being completely inundated.

This was sent to me by a well-meaning friend, and....

I got this from a friend I trust, but I was wondering if this was a valid article.

I get tired of the multiple "warnings of impending doom" that I get from many well-meaning but misguided friends, family and co-workers.

I'm trying to dispel this note that I received from my (well intentioned) father.

Personally, I dislike email chain-letters, even ones with a core of legitimacy....

I'm sick of people sending me this stuff !!!!

These correspondents have made clear to me the e-mail 'Net rumors that they receive from friends and loved ones really aren't welcome. To use an analogy, imagine if your friends treated you to large bags of catalogs and bulk rate mail every time they came over for dinner. Well, is this very different?

The inspiration seems to be that e-mail is such a convenience, sending these messages on with or without comment ("I don't know if this is true or not, but it's something to think about!") is too good an opportunity to pass up. Opportunity for what? To make contact. It takes time and effort to send an original, genuine letter. Forwarding impersonal e-mail must be the next best thing.

What's a friend to do? Be thoughtful, at the very least. Read the message, wield some healthy skepticism, check out any Web links (if any) that the message provides. If there's any remaining doubt, avail yourself of the references listed above. More than likely, you'll find that the "new, dire

warning" you've received is actually stale, old hocus. Would you still hit the FORWARD button if you knew that the message was false?

Thank you for reading this page. Please feel free to share the link to this page with anyone who sends you e-v-mail. To hear the latest in net hoaxes and online deceptions, tune in to my regular column, the "Hoax du Jour."

David Spalding

08 September 1997 Last revision: 18 September 1999

Public links to this specific article: http://korova.com/virus/.